



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,560	06/30/2000	Paul C. Drews	042390.P6758	1539

7590

07/06/2004

Blakely Sokoloff Taylor & Zafman L L P  
12400 Wilshire Boulevard Seventh Floor  
Los Angeles, CA 90025

EXAMINER

MCARDLE, JOSEPH M

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 07/06/2004

2

Please find below and/or attached an Office communication concerning this application or proceeding.

SK

# Office Action Summary

Application No.

09/608,560

Applicant(s)

DREWS, PAUL C.

Examiner

Joseph McArdle

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 30 June 2000.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-68 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-11, 13-28, 30-62 and 64-68 is/are rejected.
- 7) ☒ Claim(s) 12, 29, 46 and 63 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 June 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date: \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### *Claim Objections*

1. Claim 68 is objected to because of the following informalities: Claim 68 recites "The of system", the examiner asserts that this claim should read as "The system of". Appropriate correction is required.

### *Claim Rejections - 35 USC § 102*

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 5, 6, 9-11, 13, 14, 17, 18-20, 22, 23, 26-28, 30, 31, 34, 35-37, 39, 40, 43-45, 47, 48, 51-54, 56, 57, 60-62, 64, 65, and 68 rejected under 35 U.S.C. 102(e) as being anticipated by Vaeth (U.S. Patent No. 6308277). In regards to claims 1, 18, 35, 52 and 68, Vaeth discloses a design that is directed towards certificate authorities and their use in establishing and authenticating communications. Vaeth further discloses in column 4, lines 34-57 that a requester (a requesting platform in the present case) employs a public/private key pair generator to generate a key pair and also prepares a certificate request, which is signed (encrypted) with the private key of the requester. It is also

Art Unit: 2132

disclosed in the aforementioned location that a registration authority verifies the identity of the requester and passes the certificate request on to a certifying authority (CA). It is then disclosed in the aforementioned location that the CA uses its private key to sign the request certificate forming a signed certificate that is then passed back to the requester via secure means. These disclosures meet the limitations set forth under claims 1, 18, 35 and 52 that call for having a platform identifier unique to a platform as well as an authentication identifier (certificate) that is provided by an authentication vendor (certifying authority) using the platform identifier, a platform private key, and an authentication private key (CA private key) because the CA uses its private key to sign a certificate (authentication identifier) specific to the identity of the requester (platform) that issued the request using its private key. These disclosures also meet the limitations set forth under the aforementioned claims that call for having a signature generator to generate digital signature using the platform identifier (identity of the requesting platform) and the authentication identifier (certificate).

4. In regards to claims 14, 31, 48, and 65, Vaeth discloses a design that is directed towards certificate authorities and their use in establishing and authenticating communications. Vaeth further discloses in column 4, lines 34-57 that a requester (a requesting platform in the present case) employs a public/private key pair generator to generate a key pair and also prepares a certificate request, which is signed (encrypted) with the private key of the requester. It is also disclosed in the aforementioned location that a registration authority verifies the identity of the requester and passes the certificate request on

Art Unit: 2132

to a certifying authority (CA). It is then disclosed in the aforementioned location that the CA uses its private key to signed the request certificate forming a signed certificate that is then passed back to the requester via secure means. These disclosures meets the limitations set forth under claims 14, 31, 48 and 65 that call for encrypting a platform private key using an authentication private key because the disclosed CA's private key (authentication private key) is used to sign (encrypt) the requester's private key. These disclosures also meet the limitations set forth under the aforementioned claims that call for transforming the platform private key to generate an authentication identifier using a platform identifier and providing the authentication identifier to the platform because the CA uses its private key to sign a certificate request thereby forming a signed certificate (authentication identifier) specific to the identity if the requester, which is transmitted back to the requester.

5. In regards to claims 2, 19, 36 and 53, Vaeth discloses a design that is directed towards certificate authorities and their use in establishing and authenticating communications. Vaeth further discloses in column 4, lines 34-57 that a requester (a requesting platform in the present case) employs a public/private key pair generator to generate a key pair and also prepares a certificate request, which is signed (encrypted) with the private key of the requester. It is also disclosed in the aforementioned location that a registration authority verifies the identity if the requester and passes the certificate request on to a certifying authority (CA). It is then disclosed in the aforementioned location that the CA uses its private key to signed the request certificate forming a signed

Art Unit: 2132

certificate that is then passed back to the requester via secure means. These disclosures meet the limitations set forth under claims 2, 19, 36, and 53 that call for having a platform-specific transform to transform the authentication identifier using the platform identifier to output an encrypted platform private key because the CA issues a certificate (authentication identifier) by signing (encrypting) the requester's (requesting platform) certificate request that includes the identity of the requester as well as the private key of the requester. Vaeth further discloses in column 2, lines 33-46 that communications encrypted using a private key can be decrypted using a supplied public key. Vaeth also discloses in column 4, lines 52-53 that a copy of the CA's (authentication vendor) public key is transmitted back to the requester along with the certificate (authentication identifier) so that the requester can decrypt the signed certificate via the CA's public key in order to retrieve its own private key, which will verify the integrity and authenticity of the communication. These disclosures meet the limitations set forth under the aforementioned claims that call for decrypting the encrypted (signed) platform private key by using the public key of the authentication vendor.

6. In regards to claims 3, 20, 37 and 54, Vaeth discloses in column 4, lines 34-37 how a requester (requesting platform) can sign data with its own private key (platform private key). Also, since the requester's private key can be used by the requesting platform it is transparent to the platform. These disclosures meet the limitations set forth under claims 3, 20, 37 and 54 that call for having a signer to sign data using the platform private key that is transparent to the platform.

Art Unit: 2132

7. In regards to claims 5, 22, 39 and 56, Vaeth discloses in column 4, lines 34-57 how a copy of the CA's (authentication vendor) public key is transmitted back to the requester along with the signed certificate (authentication identifier) so that the requester can decrypt the signed certificate via the CA's public key in order to be able to retrieve its original message signed (encrypted) under its own private key, which will verify the integrity and authenticity of the communication. This disclosure meets the limitations set forth under claims 5, 22, 39 and 56 that call for decrypting the authentication identifier (certificate) with a key corresponding to the platform identifier because the original certificate request was signed (encrypted) with the requester's private key (which directly corresponds to the requester's identity) and can only be decrypted and verified by the specific requester (platform identifier) for which the certificate was intended.

8. In regards to claim 6, Vaeth discloses in column 4, lines 34-57 that a requester (a requesting platform in the present case) employs a public/private key pair generator to generate a key pair and also prepares a certificate request, which is signed (encrypted) with the private key of the requester. It is also disclosed in the aforementioned location that a registration authority verifies the identity of the requester and passes the certificate request on to a certifying authority (CA). It is then disclosed in the aforementioned location that the CA uses its private key to sign the request certificate forming a signed certificate that is then passed back to the requester via secure means. These disclosures meet the limitations set forth under the aforementioned claims that call for

Art Unit: 2132

transforming the platform private key to generate an authentication identifier using a platform identifier and providing the authentication identifier to the platform because the CA uses its private key to sign a certificate request thereby forming a signed certificate (authentication identifier) specific to the identity of the requester, which is transmitted back to the requester.

9. In regards to claims 9, 17, 26, 34, 43, 51, and 60, Vaeth discloses in column 4, lines 34-57 that the requester prepares a certificate request that is then signed with the requester's private key (a key that corresponds only to that specific requester). This disclosure meets the limitations set forth under claims 9, 17, 26, 34, 43, 51, and 60 that call for using an encryptor to encrypt (sign) the platform private key using a symmetric encryption/decryption key related to the platform identifier because the requester's private key is used to sign (encrypt) the certificate request yielding a certificate request that is signed by and includes the requester's private key (which corresponds directly with the requester's identity).

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 4, 21, 38, 55, 7, 24, 41, 58, 15, 32, 49, 66, 8, 25, 42, 59, 16, 33, 50 and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaeth in

Art Unit: 2132

view of Harkins (U.S. Patent No. 6038322). In regards to claims 4, 21, 38 and 55, Vaeth's design disclosed above meets all of the aforementioned limitations set forth under claims 2, 19, 36, and 53. However, Vaeth's design makes no mention of having an exclusive-OR device to perform an XOR function on the platform identifier and the authentication identifier. The exclusive-OR function is one such function that is frequently used to provide cryptographic manipulations. Hawkins teaches in column 5, lines 67 through column 6, lines 1-4 that the exclusive-OR function is reversible and it, or any other reversible function, can be employed to perform reversible cryptographic manipulations on sets of data. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Hawkins's teachings on the uses of the XOR function into Vaeth's design in order to achieve a design that is capable of having an exclusive-OR device for performing an XOR function on the platform identifier and the authentication identifier.

12. In regards to claims 7, 24, 41, and 58, Vaeth's design disclosed above meets all of the aforementioned limitations set forth under claims 6, 23, 40, and 57. However, Vaeth's design makes no mention of having an exclusive-OR device for performing an XOR function on the encrypted platform private key using the platform identifier. The exclusive-OR function is one such function that is frequently used to provide cryptographic manipulations. Hawkins teaches in column 5, lines 67 through column 6, lines 1-4 that the exclusive-OR function is reversible and it, or any other reversible function, can be employed to perform reversible cryptographic manipulations on sets of data. It would have been

Art Unit: 2132

obvious to one of ordinary skill in the art at the time the invention was made to combine Hawkins's teachings on the uses of the XOR function into Vaeth's design in order to achieve a design that is capable of having an exclusive-OR device for performing an XOR function on the encrypted platform private key using the platform identifier.

13. In regards to claims 15, 32, 49, and 66, Vaeth's design disclosed above meets all of the aforementioned limitations set forth under claims 14, 21, 48 and 65. However, Vaeth's design makes no mention of having an exclusive-OR device for performing an XOR function on the encrypted platform private key and the platform identifier to generate the authentication identifier. The exclusive-OR function is one such function that is frequently used to provide cryptographic manipulations. Hawkins teaches in column 5, lines 67 through column 6, lines 1-4 that the exclusive-OR function is reversible and it, or any other reversible function, can be employed to perform reversible cryptographic manipulations on sets of data. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Hawkins's teachings on the uses of the XOR function into Vaeth's design in order to achieve a design that is capable of having an exclusive-OR device for performing an XOR function on the encrypted platform private key and the platform identifier to generate the authentication identifier.

14. Claims 13, 30, 47, and 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaeth in view of Fischer (U.S. Patent No. 6289459). In regards to claims 13, 30, 47 and 64, Vaeth's design disclosed above meets all of

Art Unit: 2132

the aforementioned limitations set forth under claims 1, 18, 35, and 52.

However, Vaeth's design makes no specific mention of identifying a platform according to a serial number retrieved from the processor. Fischer teaches in column 2, lines 10-14 that a processor number is one way to provide a unique identity for a system. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Fischer's teachings on using a processor number as a means for identifying a system in order to achieve a design that is capable of having a platform identifier that consists of a processor serial number.

15. Claims 10, 11, 27, 28, 45, 46, 61 and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaeth in view of Ahuja (U.S. Patent No. 6122732). In regards to claims 10, 11, 27, 28, 45, 46, 61 and 62, Vaeth's design disclosed above meets all of the limitations set forth under claims 1, 18, 35, and 52. However, Vaeth's design makes no mention of placing the platform identifier in a protected storage environment such as the System Management Basic Input/Output System Table (SMBIOS). Ahuja teaches in column 1, lines 7-16 that SMBIOS is a protected memory area. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Ahuja's teaching relating to how SMBIOS is considered a protected memory area into Vaeth's design in order to achieve a design that is capable of storing the platform identifier in a protected memory area such as the SMBIOS for the purposes of ensuring that the platform identifier can not be altered or tampered with.

Art Unit: 2132

16. In regards to claims 8, 25, 42, 59, 16, 33, 50 and 67, the identity of the requester (platform identifier) disclosed in Vaeth's design would be represented in the present communication system as a series of bits that together would serve to identify a requester. This disclosure meets the limitations set forth under claims 8, 25, 42, 59, 16, 33, 50 and 67 that call for having a platform identifier be a serially uncorrelated bit stream.

***Allowable Subject Matter***

17. Claims 12, 29, 46, and 63 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph McArdle whose telephone number is (703) 305-7515. The examiner can normally be reached on Weekdays from 8:00 am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

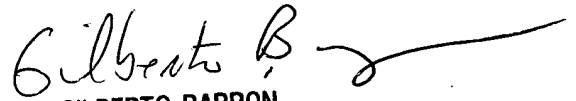
Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Joseph McArdle  
Examiner  
Art Unit 2132

jmm



GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100